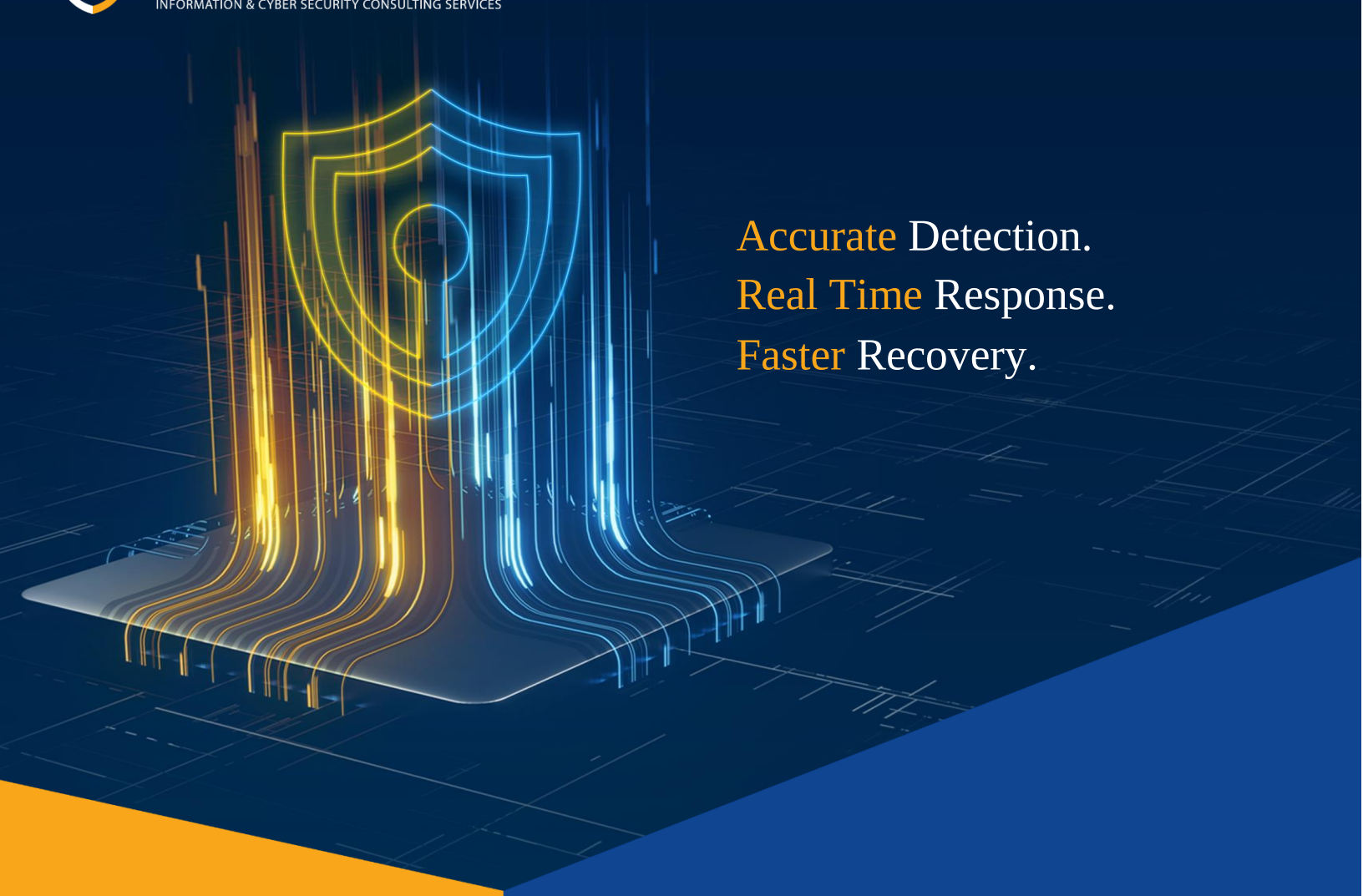
G'SECURE LABS
INFORMATION & CYBER SECURITY CONSULTING SERVICES



Accurate Detection.
Real Time Response.
Faster Recovery.

Planned list of Activities And Validation Process For Execution of VAPT

STRYKER, INDIA

stryker

April 7th, 2022

Planned list of Activities and Validation Process for Execution of VAPT

Warning: THIS DOCUMENT MAY CONTAIN INFORMATION THAT COULD SEVERELY DAMAGE OR IMPACT THE INTEGRITY AND SECURITY OF THE ORGANIZATION IF DISCLOSED PUBLICLY. THIS DOCUMENT SHOULD BE SAFEGUARDED AT ALL TIMES AND MAINTAINED IN A SECURE AREA WHEN NOT IN USE. G' SECURE LABS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR THE SECURITY OF THIS DOCUMENT AFTER DELIVERY TO THE ORGANIZATION NAMED HEREIN. IT IS THE ORGANIZATION'S RESPONSIBILITY TO SAFEGUARD THIS MATERIAL AFTER DELIVERY.

THIS REPORT CONTAINS PROPRIETARY INFORMATION THAT IS NOT TO BE SHARED, COPIED, DISCLOSED OR OTHERWISE DIVULGED WITHOUT THE EXPRESS WRITTEN CONSENT OF G' SECURE LABS OR THEIR DESIGNATED REPRESENTATIVE. USE OF THIS REPORTING FORMAT BY OTHER THAN G' SECURE LABS OR ITS SUBSIDIARIES IS STRICTLY PROHIBITED AND MAY BE PROSECUTED TO THE FULLEST EXTENT OF THE LAW.

Disclaimer: THE RECOMMENDATIONS CONTAINED IN THIS REPORT ARE BASED ON INDUSTRY STANDARD "BEST PRACTICES". BEST PRACTICES ARE, BY NECESSITY, GENERIC IN NATURE AND MAY NOT TAKE INTO ACCOUNT EXACERBATING OR MITIGATING CIRCUMSTANCES. THESE RECOMMENDATIONS, EVEN IF CORRECTLY APPLIED, MAY CAUSE CONFLICTS IN THE OPERATING SYSTEM OR INSTALLED APPLICATIONS. ANY RECOMMENDED CHANGES TO THE OPERATING SYSTEM OR INSTALLED APPLICATION SHOULD FIRST BE EVALUATED IN A NON-PRODUCTION ENVIRONMENT BEFORE BEING DEPLOYED IN THE PRODUCTION ENVIRONMENT.

G' SECURE LABS

Recipient:

Name/role	Company
Deepak	Stryker

Document Version:

Name of the Author	Version	Title	Date
Arunesh Mishra	1.0	Planned list of Activities And Validation Process For Execution of VAPT	April 7th, 2022

Table of Contents

1. Summary

Stryker has assigned the task of carrying out vulnerability assessment and penetration testing of their SmartMedic Platform by G'Secure Labs team. This is planned list of activities and validation process for execution of VAPT task. The version 1.0 detailed planned list of activities described about each validation process task. The steps or protocols which has been shared in this file according to the particular Smart medic component mentioned in the specific row with respect to the vulnerabilities mapped to the components.

2. Planned List of Activities and Validation Process

Threat Event(s)	Vulnerabilities	Asset	Planned list of Activities And Validation Process For Execution of VAPT
Deliver undirected malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.

Deliver undirected malware (CAPEC-185)	External communications and exposure for communciation channels from and to application and devices like tablet and smartmedic device.	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	External communications and exposure for communciation channels from and to application and devices like tablet and smartmedic device.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Legacy system identification if any	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected	Legacy system identification if any	Tablet Resources - web cam, microphone, OTG devices,	1) Create Android malware 2) Transfer the malware to

malware (CAPEC-185)		Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Device Maintainence tool (Hardware/Software)	NA
Deliver undirected malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities

			8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Lack of plan for periodic Software Vulnerability Management	Device Maintainence tool (Hardware/Software)	NA
Deliver undirected malware (CAPEC-185)	Lack of plan for periodic Software Vulnerability Management	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Lack of plan for periodic Software Vulnerability Management	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning

			for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unencrypted data at rest in all possible locations	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 9) Use sniffing tool to sniff the data at motion and MITM
Deliver undirected malware (CAPEC-185)	Unencrypted data in flight in all flowchannels	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning

			for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unencrypted data in flight in all flowchannels	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Outdated - Software/Hardware	Device Maintainence tool (Hardware/Software)	NA
Deliver undirected malware (CAPEC-185)	Outdated - Software/Hardware	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Outdated - Software/Hardware	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information

			gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Device Maintainence tool (Hardware/Software)	NA
Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Wireless Network device	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to

			vulnerability 5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering. 8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Deliver directed malware (CAPEC-185)	External communications and exposure for communciation channels from and to application and devices like tablet and smartmedic device.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.

			7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Device Maintainence tool (Hardware/Software)	NA
Deliver directed malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability

			5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Wireless Network device	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering. 8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while

			VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unencrypted data at rest in all possible locations	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 9) Use sniffing tool to sniff the data at motion and MITM
Deliver directed malware (CAPEC-185)	Unencrypted data at rest in all possible locations	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning

			for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 9) Use sniffing tool to sniff the data at motion and MITM
Deliver directed malware (CAPEC-185)	Unencrypted data at rest in all possible locations	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Use sniffing tool to sniff the data at motion and MITM
Gaining Access ([S]TRID[E])	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Gaining Access ([S]TRID[E])	Unprotected network port(s) on network devices and connection points	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Unprotected network port(s) on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device

		Application, Network interfaces (Bluetooth, Wifi)	4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Gaining Access ([S]TRID[E])	Devices with default passwords needs to be checked for bruteforce attacks	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Devices with default passwords needs to be checked for bruteforce attacks	Interface/API Communication	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools.

			4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Checking authentication modes for possible hacks and bypasses	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali

			tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Checking authentication modes for possible hacks and bypasses	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Checking authentication modes for possible hacks and bypasses	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Controlled Use of Administrative Privileges over the network	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port

Gaining Access ([S]TRID[E])	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Maintaining Access (TTP)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.

Maintaining Access (TTP)	Devices with default passwords needs to be checked for bruteforce attacks	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Maintaining Access (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.

			5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Maintaining Access (TTP)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	Controlled Use of Administrative Privileges over the network	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.

			5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Clearing Track (TTP)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Clearing Track (TTP)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Clearing Track (TTP)	Outdated - Software/Hardware	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.

Clearing Track (TTP)	Lack of configuration controls for IT assets in the informaion system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Clearing Track (TTP)	Lack of configuration controls for IT assets in the informaion system plan	Device Maintainence tool (Hardware/Software)	NA
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Device Maintainence tool (Hardware/Software)	NA
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability

			5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Clearing Track (TTP)	The static connection digaram between devices and applications with provision for periodic updation as per changes	Device Maintainence tool (Hardware/Software)	NA
Clearing Track (TTP)	The static connection digaram between devices and applications with provision for periodic updation as per changes	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Elevation of privilege (STRID[E])	Controlled Use of Administrative Privileges over the network	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the

			authentication/authorization on the open port
Elevation of privilege (STRID[E])	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Denial of service (STRI(D)E)	Unprotected network port(s) on network devices and connection points	Wireless Network device	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering. 8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools.
Denial of service (STRI(D)E)	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Information disclosure (STR(I)DE)	Unencrypted data at rest in all possible locations	Data at Rest	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.

			2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM 8) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	Unencrypted data in flight in all flowchannels	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	Weak Encryption Implementaion in data at rest and in motion tactical and design wise	Data at Rest	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.

			5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	Weak Encryption Implementaion in data at rest and in motion tactical and design wise	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	Weak Algorthim implementation with respect cipher key size	Data at Rest	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM

Information disclosure (STR(I)DE)	Weak Algorthim implementation with respect cipher key size	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Information disclosure (STR(I)DE)	Unencrypted Network segment throught the information flow	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port

			6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	Insecure communications in networks (hospital)	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Data Access (STR[I]DE)	Unprotected network port(s) on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Data Access (STR[I]DE)	Unprotected network port(s) on network devices and connection points	Wireless Network device	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports

			6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering. 8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools.
Data Access (STR[I]DE)	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Data Access (STR[I]DE)	Devices with default passwords needs to be checked for bruteforce attacks	Data at Rest	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Data Access (STR[I]DE)	Devices with default passwords needs to be	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.

	checked for bruteforce attacks		2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Data Access (STR[I]DE)	Devices with default passwords needs to be checked for bruteforce attacks	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Data Access (STR[I]DE)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Data at Rest	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force

			attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Data Access (STR[I]DE)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Data Access (STR[I]DE)	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Data Access (STR[I]DE)	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Open network port exploit (TTP)	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports

			6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Open network port exploit (TTP)	Unprotected network port(s) on network devices and connection points	Wireless Network device	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering. 8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools.
Open network port exploit (TTP)	Unencrypted Network segment throught the information flow	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Open network port exploit (TTP)	Unencrypted Network segment throught the information flow	Wireless Network device	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports

			6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering. 8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools.
Open network port exploit (TTP)	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Open network port exploit (TTP)	Unencrypted data in flight in all flowchannels	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Open network port exploit (TTP)	Insecure communications in networks (hospital)	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while

			assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Brute-force Attack (CAPEC-112)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Devices with default passwords needs to be checked for bruteforce attacks	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Brute-force Attack (CAPEC-112)	The password complexity or location vulnerability. Like	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.

	weak passwords and hardcoded passwords.		2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Brute-force Attack (CAPEC-112)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Checking authentication modes	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.

	for possible hacks and bypasses		2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Weak Encryption Implementaion in data at rest and in motion tactical and design wise	Data at Rest	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Brute-force Attack (CAPEC-112)	Weak Encryption Implementaion in data at rest and in motion tactical and design wise	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM

Social Engineering (TTP)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	Legacy system identification if any	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Interface/API Communication	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali

			tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Lack of evidence to conclude any malicious attempt/attack (ST[R]IDE)	Insufficient Logging information	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Lack of evidence to conclude any malicious attempt/attack (ST[R]IDE)	Insufficient Access permissions for accessing and modifying Log files	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali

			tools. 4) Exploit the open ports using kali tools.
Unauthorized Alterations (S[T]RIDE)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Unauthorized Alterations (S[T]RIDE)	Insufficient Access permissions for accessing and modifying Log files	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Error Info containing sensitive data for Failed Authentication attempts	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.

Gaining Access ([S]TRID[E])	Error Info containing sensitive data for Failed Authentication attempts	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Absence of additional security factor along with user identification	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Absence of additional security factor along with user identification	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Having no limit on the login attempts	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.

			2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Having no limit on the login attempts	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Brute-force Attack (CAPEC-112)	Error Info containing sensitive data for Failed Authentication attempts	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Error Info containing sensitive data for Failed Authentication attempts	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port

			6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Brute-force Attack (CAPEC-112)	Absence of additional security factor along with user identification	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Absence of additional security factor along with user identification	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Brute-force Attack (CAPEC-112)	Having no limit on the login attempts	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Having no limit on the login attempts	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while

			VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port

*** End of the document

G'SECURE LABS
INFORMATION & CYBER SECURITY CONSULTING SERVICES

THE NETHERLAND
Maria Montessorilaan 3,
2719 DB Zoetermeer,
The Netherlands

INDIA
B/81, Corporate House,
Judges Bungalow Road, Bodakdev,
Ahmedabad - 380054. India

www.gsecurelabs.com